

MIKOS-101  
Amendment dated 02/11/2005

09/778,967

07650001aa  
Reply to office action mailed 08/11/2004

The following is a complete listing of all claims in the application, with an indication of the status of each:

**Listing of claims:**

- 1        1. (currently amended) System for authenticating digital information,  
2        comprising:
  - 3                a) an image acquisition device for producing an original array of  
4        two-dimensional digital information;
  - 5                b) means for obtaining current date and time information from satellite  
6        or radio broadcasts;
  - 7                c) means for obtaining current location information from satellite or  
8        radio broadcasts;
  - 9                d) means for identifying a Sensor ID for the image acquisition device;
  - 10              e) an encoder for converting date/time, location, and Sensor ID into  
11        two-dimensional format called the Encoded Data Array;
  - 12              f) an embedder for combining the Encoded Data Array and the  
13        Original Array into a new Composite Array
  - 14              ~~g) an encrypter for transforming the Composite Array into another~~  
15        ~~two-dimensional array called the Encrypted Composite Array;~~
  - 16              h) a Transmission ~~Process~~ device to transfer the ~~Encrypted~~ Composite  
17        Array to ~~the intended~~ a recipient;
  - 18              ~~i) a decrypter to restore the Composite Array~~
  - 19              n) means for comparing said transferred Composite Array to said  
20        Encoded Data Array, said comparing means thereby being able to determine  
21        whether said Encoded Data Array is embedded in said Composite Array;
  - 22              j) a decoder with fault indicator when date/time, location, and source  
23        cannot be decoded;

MIKOS-101  
Amendment dated 02/11/2005

09/778,967

07650001aa  
Reply to office action mailed 08/11/2004

24 k) an Encoding Extractor for removing the Encoded Data Array from  
25 the ~~Decrypted~~ Composite Array;  
26 l) means for restoring the Original Array at pixel locations used for the  
27 Encoding; and  
28 m) means for determining changes between the Restored Original  
29 Array and the Original Array.

1 2. (currently amended) System as in Claim 1 in which the Original Array  
2 size is increased by a factor and subpixels are used in steps ~~f through~~ h, n, j,  
3 k, l, and m.

1 3. (currently amended) System as in ~~Claims 1 and 2~~ claim 20 in which the  
2 encryption of step g and decryption of step i is repeated more than one time.

1 4. (currently amended) System as in Claims 1 ~~and or~~ 2 in which the  
2 encryption process involves scrambling the pixels or subpixels.

1 5. (currently amended) System as in Claims 1 ~~and or~~ 2 in which steps b and c  
2 utilize the GPS (Global Positioning Satellite) system.

1 6. (currently amended) System as in Claims 1 ~~and or~~ 2 in which the Decoder  
2 utilizes ~~Flash Correlation~~ flash correlation to select pixel locations of the  
3 Encoded Data Array and test for authenticity.

1 7. (currently amended) System as in Claims 1 ~~and or~~ 2 in which the Sensor  
2 ID in step d includes a biometric identifier of the User of the image  
3 acquisition device.

MIKOS-101

09/778,967

07650001aa

Amendment dated 02/11/2005

Reply to office action mailed 08/11/2004

1        8. (currently amended) System as in Claims 1 ~~and~~or 2 in which the Sensor  
2        ID in step d includes the serial number and odometer setting of the image  
3        acquisition device of step a.

1        9. (currently amended) System as in Claims 1 ~~and~~or 2 in which the change  
2        detector of step m evaluates subsections of the Restored Original Array and  
3        the Original Array to localize areas of difference.

1        10. (currently amended) System as in Claim 6 in which ~~FlashCorrelation~~  
2        flash correlation is used to verify that the encoded data is the same as data  
3        which is expected to be encoded into a particular Original Array.

1        11. (currently amended) System as in Claim 6 in which ~~FlashCorrelation~~  
2        flash correlation is used to identify the encoded data by exhaustive  
3        comparison against each possible value for each of date/time, location, and  
4        source.

1        12. (currently amended) System as in Claims 1 ~~and~~or 2 in which date/time,  
2        location, and source are annotated onto the Encrypted Composite Array.

1        13. (currently amended) System as in Claims 1 ~~and~~or 2 in which the  
2        encoded data provides the key to the encryption and decryption algorithms.

1        14. (currently amended) System of Claims 1 ~~and~~or 2 in which the operation  
2        of the ~~EIS~~image acquisition device is triggered by the change of status of  
3        another device.

MIKOS-101  
Amendment dated 02/11/2005

09/778,967

07650001aa  
Reply to office action mailed 08/11/2004

- 1        15. (original) System of Claim 14 in which the triggering device is a face  
2        recognition system.
- 1        16. (original) System of Claim 14 in which the triggering device is a speed  
2        sensor.
- 1        17. (original) System of Claim 14 in which the triggering device is an alarm  
2        condition sensor.
- 1        18. (currently amended) System of Claims 1 ~~and or~~ 2 in which the Encoding  
2        is performed by overlaying a pattern of pixels of a particular color or grey  
3        scale value.
- 1        19. (currently amended) System of Claims 1 ~~and or~~ 2 in which the Encoding  
2        is performed by steganography.
- 1        20. (currently amended) System of Claims 1 ~~and or 2 in which no encryption~~  
2        ~~or scrambling is performed, further comprising:~~  
3                g) an encrypter for encrypting the Composite Array;  
4                i) a decrypter to restore the Composite Array.
- 1        21. (original) A method for authenticating digital images, comprising the  
2        steps of:  
3                capturing a digital image;  
4                recording authentication information at the time and place of said  
5        capturing, said authentication information being unique to said digital image  
6        and including at least one piece of information from a source independent of  
7        said capturing;

MIKOS-101  
Amendment dated 02/11/2005

09/778,967

07650001aa  
Reply to office action mailed 08/11/2004

8            encoding said authentication information into a data array mapable to  
9            said digital image;  
10           mapping said data array to said digital image, thereby creating a  
11           composite array;  
12           optionally encrypting said composite array;  
13           optionally annotating said composite array;  
14           comparing said data array, optionally encrypted and annotated, to a  
15           target composite array, wherein said comparing determines whether said  
16           authentication information is embedded in said target composite array,  
17           thereby proving that said target composite array is an authentic copy of said  
18           composite array.

1           22. (original) The method of claim 21, wherein said at least one piece of  
2           information from a source independent of said capturing is GMT time  
3           information.

1           23. (original) The method of claim 21, wherein said at least one piece of  
2           information from a source independent of said capturing is GPS location  
3           information.

1           24. (original) The method of claim 21, wherein said at least one piece of  
2           information from a source independent of said capturing is GMT time  
3           information and GPS location information.

1           25. (currently amended) The method of claim 21, wherein said comparing  
2           step is ~~flash correlation~~ flash correlation of said data array with said target  
3           composite array.

MIKOS-101  
Amendment dated 02/11/2005

09/778,967

07650001aa  
Reply to office action mailed 08/11/2004

1        26. (currently amended) The method of claim 25, wherein said digital image  
2        is a sequence of digital images, there being a unique set of authenticating  
3        information for each digital image in said sequence and a corresponding  
4        unique data array, there being a unique composite array corresponding to each  
5        digital image in said sequence, wherein said composite array is a sequence of  
6        composite arrays and said target composite array is a sequence of target  
7        composite arrays, and wherein said ~~flash correlation~~ flash correlation  
8        determines whether said sequence of target composite arrays is an authentic  
9        copy of said sequence of composite arrays.

1        27. (currently amended) The method of claim 26, wherein said sequence of  
2        digital images is a video image and said ~~flash correlation~~ flash correlation is  
3        done in real time.

1        28. (original) A system for authenticating digital images, comprising:  
2                means for capturing a digital image;  
3                means for recording authentication information at the time and place  
4        of said capturing, said authentication information being unique to said digital  
5        image and including at least one piece of information from a source  
6        independent of said capturing;  
7                means for encoding said authentication information into a data array  
8        mapable to said digital image;  
9                means for mapping said data array to said digital image, thereby  
10        creating a composite array;  
11                means for optionally encrypting said composite array;  
12                means for optionally annotating said composite array;  
13                means for comparing said data array, optionally encrypted and  
14        annotated, to a target composite array, wherein said comparing determines

MIKOS-101  
Amendment dated 02/11/2005

09/778,967

07650001aa  
Reply to office action mailed 08/11/2004

15        whether said authentication information is embedded in said target composite  
16        array, thereby proving that said target composite array is an authentic copy of  
17        said composite array.

1        29. (original) The system of claim 28, wherein said at least one piece of  
2        information from a source independent of said capturing is GMT time  
3        information.

1        30. (original) The system of claim 28, wherein said at least one piece of  
2        information from a source independent of said capturing is GPS location  
3        information.

1        31. (original) The system of claim 28, wherein said at least one piece of  
2        information from a source independent of said capturing is GMT time  
3        information and GPS location information.

1        32. (currently amended) The system of claim 28, wherein said comparing  
2        step is ~~flash correlation~~ flash correlation of said data array with said target  
3        composite array.

1        33. (currently amended) The system of claim 32, wherein said digital image  
2        is a sequence of digital images, there being a unique set of authenticating  
3        information for each digital image in said sequence and a corresponding  
4        unique data array, there being a unique composite array corresponding to each  
5        digital image in said sequence, wherein said composite array is a sequence of  
6        composite arrays and said target composite array is a sequence of target  
7        composite arrays, and wherein said ~~flash correlation~~ flash correlation

MIKOS-101

09/778,967

07650001aa

Amendment dated 02/11/2005

Reply to office action mailed 08/11/2004

8 determines whether said sequence of target composite arrays is an authentic  
9 copy of said sequence of composite arrays.

1 34. (currently amended) The system of claim 33, wherein said sequence of  
2 digital images is a video image and said ~~flash correlation~~ flash correlation is  
3 done in real time.